

01-16-01

526 Rec'd PCT/PTO

12 JAN 2001

FORM PTO-1390
(REV 11-2000)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371

CH919980027US1

U.S. APPLICATION NO. 01/km/1/37/CF/1/5

09/743844

INTERNATIONAL APPLICATION NO.

PCT/IB98/01854

INTERNATIONAL FILING DATE

23 November 1998

PRIORITY DATE CLAIMED

15 July 1998

TITLE OF INVENTION METHOD OF ESTABLISHING THE TRUSTWORTHINESS LEVEL OF A
PARTICIPANT IN A COMMUNICATION CONNECTION

APPLICANT(S) FOR DO/EO/US

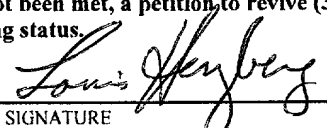
Carl Binding et al

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
 - a. ☐ is attached hereto (required only if not communicated by the International Bureau).
 - b. ☒ has been communicated by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
 - a. ☐ is attached hereto.
 - b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. ☐ are attached hereto (required only if not communicated by the International Bureau).
 - b. ☐ have been communicated by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A **FIRST** preliminary amendment.
14. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information: A copy of form PCT/IB/308

U.S. APPLICATION NO. (if known, see 37 CFR 1.5) 09/743844		INTERNATIONAL APPLICATION NO. PCT/IB98/01854		ATTORNEY'S DOCKET NUMBER CH919980027US1	
21. <input type="checkbox"/> The following fees are submitted: BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)): Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO. \$1000.00 International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO \$860.00 International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$710.00 International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) \$690.00 International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) \$100.00 ENTER APPROPRIATE BASIC FEE AMOUNT =				CALCULATIONS PTO USE ONLY	
Surcharge of \$130.00 for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				\$860.00	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	\$	
Total claims	22 - 20 =	2	x \$18.00	\$ 36.00	
Independent claims	4 - 3 =	1	x \$80.00	\$ 80.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)				+ \$270.00	
TOTAL OF ABOVE CALCULATIONS =				\$946.00	
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.				\$	
SUBTOTAL =				\$	
Processing fee of \$130.00 for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				\$	
TOTAL NATIONAL FEE =				\$	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property +				\$	
TOTAL FEES ENCLOSED =				\$946.00	
				Amount to be refunded:	\$
				charged:	\$
a. <input type="checkbox"/> A check in the amount of \$ _____ to cover the above fees is enclosed. b. <input checked="" type="checkbox"/> Please charge my Deposit Account No. <u>09-0468</u> in the amount of \$ <u>946.00</u> to cover the above fees. A duplicate copy of this sheet is enclosed. c. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. <u>09-0468</u> . A duplicate copy of this sheet is enclosed. d. <input type="checkbox"/> Fees are to be charged to a credit card. WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.					
NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.					
SEND ALL CORRESPONDENCE TO					
 SIGNATURE Louis P. Herzberg NAME 41,500 REGISTRATION NUMBER					

METHOD OF ESTABLISHING THE TRUSTWORTHINESS LEVEL OF A PARTICIPANT IN A COMMUNICATION CONNECTION

The invention relates to a method for establishing a trustworthiness level of a participant in a communication connection between a first communication partner and a second communication partner. More particularly it relates to a method for establishing the trustworthiness level of a handheld device, such as a handheld telephone in a trusted environment, e.g. comprising a smartcard and a back-end server.

TECHNICAL FIELD AND BACKGROUND OF THE INVENTION

Integrated-circuit cards, also known as smartcards, are generally believed to offer more tamper resistance than conventional computer systems, and are thus frequently used for authentication and security functions within large computer systems. As an example, the use of a smartcard as the Subscriber Identification Module, short SIM, within the GSM mobile-telephony system is considered. Here, the mobile handset, also called mobile equipment or ME, is not normally considered as a trusted device and a trusted smartcard is used to securely store and process subscriber information and authentication functions. When placing a call, the mobile network authenticates the mobile user by exercising authentication functions contained in the trusted smartcard.

Handheld phones are currently being extended to allow user programs to be executed on the handheld phone for value-add applications such as banking and payment. Access to the smartcard of the handheld phone is provided for the relevant security functions required for a value-add application, such as the initial authentication for a financial transaction originating from the handset. While it is possible to have the smartcard perform all critical security functions, this is unlikely since the smartcard has limited processing- and storage capacity. It is thus anticipated that security functions for complex applications like banking will not be executed solely on the smartcard, and at least partial trust must be delegated to the handheld phone. Apart from issues of processing and storage, the smartcard must implicitly trust the handheld phone to provide a reliable communication channel to and from the smartcard.

Henceforth, it is anticipated that portions of complex applications will be executed on the handheld phone. Since the handheld phone also conveys all communications between the

smartcard, the user, and the back-end server, a malicious handheld phone could conceivably alter the contents of the data packets sent between the three parties. Relying on the trusted smartcard to sign or authenticate messages does not alleviate this threat since the smartcard cannot verify that a message presented to it by the handheld phone for signature or authentication is in fact the message presented by the handheld phone to the user.

It is therefore necessary for applications that demand high levels of security and secrecy to extend the sphere of trust to include the handheld phone itself. Conventionally, this is achieved through two primary means, tamper-resistant hardware and ensuring that such tamper-resistant devices are being used through either policy or by authentication from the back-end server.

US Patent 5,371,794 discloses a method and apparatus for privacy and authentication in wireless networks. The method and apparatus is for providing a secure wireless communication link between a mobile nomadic device and a base computing unit. A mobile sends a host certificate (Cert__Mobile) to the base along with a randomly chosen challenge value (CH1) and a list of supported shared key algorithms ("SKCS"). The base determines if the Cert__Mobile is valid. If the Cert__Mobile is not valid, then the base unit rejects the connection attempt. The base then sends a Cert__Base, random number (RN1) encrypted in mobile's public key and an identifier for the chosen SKCS to the mobile. The base saves the RN1 value and adds the CH1 value and the chosen SKCS to messages sent to the base. The mobile unit then validates the Cert__Base, and if the certificate is valid, the mobile verifies under the public key of the base (Pub__Base) the signature on the message. The signature is verified by taking the base message and appending it to CH1 and the list of shared key algorithms that the mobile provided in the first message. If the base signature is not valid, then the communication attempt is aborted. In the event that the base signature is valid, the mobile determines the value of RN1 by decrypting Pub__Mobile, RN1 under the private key of the mobile. The mobile then generates RN2 and the session key, and encrypts RN2 under the Pub__Base. The mobile sends the encrypted RN2 and E(Pub__Mobile, RN1) to the base. The base then verifies the mobile signature using the Pub__Mobile obtained from the Cert__Mobile. If the mobile signature is verified, the base decrypts E(Pub__Base, RN2) using its private key. The base then determines the session key. The mobile and base may

then enter a data transfer phase using encrypted data which is decrypted using the session key which is $RN1 \oplus RN2$.

The European patent application 0 589 022 A1 discloses a public key cryptographic system with enhanced digital signature certification which authenticates the identity of the public
5 key holder. A hierarchy of nested certifications and signatures are employed which indicate the authority and responsibility levels of the individual whose signature is being certified. The certifier in constructing a certificate generates a special message that includes fields identifying the public key which is being certified, and the name of the certifier. The certificate is constructed by the certifier to define the authority which is being granted and which
10 may relate to wide range of authorizations, delegation responsibilities or restrictions given to, or placed on the certifier.

Designing special tamper-resistant hardware may involve special ruggedized designs with circuitry that erases security-sensitive information such as cryptographic parameters and aborts pending transactions if a device is physically tampered with, such as when the case is
15 opened, or the power is cut, or designing hardwired circuits that do not have any software-controlled components on the paths between the trusted smartcard and the required input/output devices.

Unfortunately, mobile equipment such as mobile handsets are not currently designed to be tamperproof and adding full tamper-resistance is not realistic for commodity-style handsets
20 due to the expected cost of doing so.

OBJECT AND ADVANTAGES OF THE INVENTION

It is an object of the invention according to claim 1 or 10 to provide a method for establishing the trustworthiness level of a participant in a communication connection in order to adapt the communication behavior to this trustworthiness level. Since the world of participants in communication is split up into tamperproof devices which can be trusted and
25 devices which are better not trusted for security-sensitive communication, the invention provides an advantageous solution for communicating between two partners over a participant by establishing its trustworthiness level and adapting the communication behavior to the established trustworthiness level. With this method, trusted and non-trusted devices can

participate in the communication and the trustworthiness of each participating device is checked automatically before communicating security-sensitive information.

behavior according to the trustworthiness level TL given in the trustworthiness level token TLT.

The smartcard 1 is then instructed by the user to establish a secure and authenticated session with the back-end server 3 so as to run the application A. The back-end server 3 and the smartcard 1 run WTLS using the option where both the client, i.e. the smartcard 1, and the back-end server 3 are authenticated using certificate exchange. At this point the trustworthiness between the back-end server 3 and smartcard 1 has been established.

When the smartcard 1 is required to send application data D to the back-end server 3, the smartcard 1 appends the trustworthiness level token TLT and sends the pair (D, TLT). Since the channel between the back-end server 3 and the smartcard 1 is authenticated, the back-end server 3 believes that the trustworthiness level TL given in the trustworthiness level token TLT is in fact the trustworthiness level TL of the handheld phone 2 hosting the smartcard 1 for this session.

The trustworthiness level token TLT is a data item which is meaningful to the back-end server 3. It could be identical with the integer value of the trustworthiness level TL, in which case the back-end server 3 shall examine the policy 16 that describes its actions or communication behavior for that trustworthiness level TL. Alternatively, the trustworthiness level token TLT could directly denote the intended trustworthiness level TL according to some relevant trustworthiness metric e.g. monetary amount. Then, no policy 16 is needed.

This example also makes the authentication step between the smartcard 1 and the back-end server 3 explicit, but this need not always be the case. If the handheld phone 2 is a GSM handset, then the smartcard 1 may be a SIM which is authenticated at the time of insertion into the handset 2 using the standard GSM authentication algorithms. The base station of the SIM could forward this authentication information to the back-end server 3, and thus eliminate the need for the establishment of WTLS session between the back-end server 3 and the SIM.

Another example is when the participant 2 does simply have stored the participant private key 8 and has no trustworthiness certificate 6. Then, the smartcard 1 can know either the participant private key 8 or the corresponding participant public key 7 and perform the above described challenge-response test to find out whether the handheld phone 2 knows the participant private key 8. If this is the case, then a corresponding trustworthiness level TL

can be assigned. Different trustworthiness levels TL can correspond to different participant private keys 8.

In the above description, the untrusted party is a phone handset. It is to be noted that the general untrusted device is simply any mobile equipment, of which a mobile handset is an
5 example.

0943460

The participant can e.g. be a mobile equipment such as a handheld phone. The trustworthiness level of the handheld phone indicates the degree of inherent tamper resistance. The first communication partner can be for instance a smartcard and the second communication partner a back-end server.

- 5 The smartcard can use the handheld phone to connect to a back-end server, and the smartcard and the back-end server are in an advantageous manner able to establish an authenticated session, assuming an untrusted handheld phone. After establishing the trustworthiness level, the smartcard communicates the trustworthiness level of the handheld phone to the back-end server without the back-end server directly authenticating the handheld phone.
- 10 It is another object to provide a method where a trustworthiness policy is specified for an application, which policy restricts the functionality of the application based on the trustworthiness level of the handheld phone.

- When the trustworthiness certificate arrives at the first communication partner signed with a signature, produced with a certificate authority private key, and the first communication
- 15 partner authenticates the signature using a certificate authority public key, a secure method is used to check whether the signature has been issued by a competent and to-be-trusted certificate authority. This is advantageous because it then can easily be confirmed that the information contained in the corresponding participant certificate is as issued by its originator.

- 20 The certificate authority public key can be read from a storage of the first communication partner, which has the advantage that this key is already available and need not be acquired from somewhere else. This also saves time.

- Communicating the detected trustworthiness level can occur by piggybacking and signing necessary information onto application level messages between the smartcard and the back-
- 25 end, application server. When the first communication partner communicates the established trustworthiness level to the second communication partner by piggy-backing a trustworthiness level information onto a communication message, signing the communication message with a first-partner private key and sending it to the second communication partner, again a very secure way of informing the back-end server about the established trustworthiness level

is chosen. Hence, a malicious participant can not amend this information and thereby pretend to be a trustable participant.

As one of the parameters of the communication behavior which is chosen in dependence of the established trustworthiness level, can be chosen the amount or number of a valuable asset, e.g. a maximum number of financial transactions and/or a maximum financial value of
5 a financial transaction and/or a maximum number of confidential words. This adapted behavior can be used to compensate for eventual lack of security which has been established in form of a low trustworthiness level. For instance, in case of a low trustworthiness level, only financial transactions up to a fixed amount of money can be executed.

10 The test whether the trustworthiness certificate belongs to the participant can be performed in that a test number is transmitted by the first communication partner to the participant from where the test number returns signed under use of the participant private key. The signature of the returning test number is verified by using a participant public key which corresponds to the participant private key. This challenge-response principle provides a
15 simple method which is easy to implement and provides a high level of security.

The participant public key can be received by the first communication partner as content of the trustworthiness certificate. This method provides for the possibility of multiple trustworthiness certificates and hence also multiple trustworthiness levels, if each certificate is assigned a different trustworthiness level.

20 When the trustworthiness level is established in that for each trustworthiness level a different trustworthiness certificate with a corresponding pair of participant public key and participant private key is used, a very simple and straightforward scheme for realizing different levels is provided. It can be used in that e.g. for different key lengths or just different signing authorities, different trustworthiness levels can be assigned.

25 The handheld phone is providing communication- and processing resources for the smartcard and the back-end server to execute an application. The back-end server wishes to authenticate the handheld phone since security-sensitive data may be sent to the smartcard via the handheld phone. As the handheld phone and the back-end server may be separated by a substantial physical distance and/or connected by a low-bandwidth network, running a
30 traditional authentication protocol between the handheld phone and the back-end server may be costly. It is hence more efficient to make use of the smartcard to authenticate the

trustworthiness level of the handheld phone locally where communication between the smartcard and handheld phone is relatively fast and cheap.

The proposed solution is most advantageous to the deployment of banking services based on mobile handsets, for example GSM telephones, since such applications demand high levels of security. As pointed out above, this in turn requires some trustworthiness level to be extended to the handset itself. Not all handsets will be trusted, due to the cost of designing and manufacturing such handsets and due to the large number of handsets which are already in-the-field that do not include any tamper-resistance.

The smartcard acts as a sort of delegate or proxy for the back-end server which establishes the trustworthiness level locally with respect to the handheld-phone/smartcard environment. The system described herein allows the trusted smartcard to detect the level of tamper-resistance of the handheld phone and communicate that level to the back-end server. An inherent advantage of the proposed solution compared to server-based device authentication methods lies in the reduced communications requirement between the back-end server and the handheld phone which lowers communications cost on one side and allows the process to be executed repeatedly if necessary, e.g., prior to each message between the smartcard and the back end server, offering additional protection.

Adapting the application behavior to the communicated trustworthiness level can be implemented by limiting the number of transactions or establishing a maximum financial value of the executed transactions. For example, from completely untrusted handsets only account inquiries might be allowed, whereas completely trusted handsets can be used to execute arbitrarily large value transactions. Handsets that offer intermediate levels of trustworthiness might be limited to transactions up to a certain value per month.

SUMMARY OF THE INVENTION

A method is proposed whereby a trustworthiness level is assigned to a handheld phone, that reflects the level of tamper-resistance that the handheld phone offers. Current mobile handsets, for example, offer no tamper-resistance and would be assigned the lowest trustworthiness level. Future fully tamperproof handsets would be assigned the highest trustworthiness level. Intermediate trustworthiness levels would designate for which incomplete but not insignificant measures against tampering have been made.

The first communication partner, e.g. a smartcard, has means of verifying the level of tamper-resistance of the handheld phone which is a participant in the communication connection between the first communication partner and a second communication partner and further has means to securely communicate the detected level of tamper-resistance in the
5 handheld phone to the second communication partner, e.g. a back-end server with whom the smartcard is communicating during the execution of an application on the participant.

The back-end server is then able to adapt the behavior of the communication, respectively application according to the level of tamper-resistance detected and communicated to it by the smartcard.

10 The basic steps of the method can be described as follows:

When the smartcard is inserted into the handheld phone to initiate a session, the smartcard requests the trustworthiness level from the handheld phone. The trustworthiness level may be assigned for example by the manufacturer of the handheld phone or perhaps by the institution with which applications on the handheld phone will communicate with or on behalf of,
15 such as a bank or credit card company.

The smartcard verifies that the trustworthiness level received from the handheld phone is valid in the sense that the token was produced by an entity with the authority to assign trustworthiness levels and also that the trustworthiness level is not being replayed. If the trustworthiness level fails verification then the handheld phone is considered untrusted. If this is
20 the case, the smartcard may choose to terminate the session, or continue the session with the restriction that only applications requiring an untrusted handheld phone can be executed. The smartcard then forms a trustworthiness level token TLT which the smartcard will use to forward to third parties to demonstrate the trustworthiness level of the handheld phone.

An application on the handheld phone is selected for execution, where the application uses
25 the network to contact a back-end server. The back-end server and the smartcard are authenticated to each other using a protocol that does not depend on the trustworthiness of the handheld phone. For example, if the handheld phone is a GSM handset and the smartcard is a SIM, then the back-end server and the smartcard SIM are authenticated using the standard GSM authentication functions. Alternatively the authentication functions of WTLS
30 can be used.

09743844-080901

The smartcard communicates the trustworthiness level of the handheld phone to the back-end server by appending the trustworthiness level token TLT to the application packets of the application that are sent from the smartcard to the back-end server S. The trustworthiness level token TLT may be appended to each packet or according to another strategy
5 depending on some policy.

Once the back-end server has received the trustworthiness level token TLT of the handheld phone via the smartcard, it need not verify the trustworthiness level of the handheld phone with the handheld phone itself, as this has been done by the trusted smartcard. The back-end server consults a trustworthiness policy which describes what restrictions are placed on
10 application relative to the trustworthiness level designated by trustworthiness level token TLT. The back-end server adjusts its actions and responses in application accordingly.

DESCRIPTION OF THE DRAWINGS

An example of the invention is depicted in the drawing and described in detail below by way of example. It is shown in fig. 1 a system with a first communication partner, a participant
15 and a second communication partner.

The figure is for sake of clarity not shown in real dimensions, nor are the relations between the dimensions shown in a realistic scale.

DETAILED DESCRIPTION OF THE INVENTION

In the following, the various exemplary embodiments of the invention are described.

20 In figure 1, a system comprising a first communication partner 1 in form of a smartcard, a second communication partner in form of a back-end server 3 and a participant 2 in a communication connection between the communication partners 1, 3 in form of a handheld phone is depicted. The handheld phone 2 comprises a memory unit 4, also called phone trustworthiness module, in which a trustworthiness certificate 6 is stored.

25 When the smartcard 1 is inserted into the handheld phone 2 to initiate a session via the communication connection, the smartcard 1 requests the transmission of the trustworthiness certificate 6 from the handheld phone 2.

The following realization is based on the use of the principle of public key cryptography, which enables an entity to produce a digital signature and other entities to verify the signature. Other authentication methods however apply as well.

It is assumed that the valid set of trustworthiness levels TL is represented by a list of L+1 integers 0, 1, ..., L, such that 0 designates no trustworthiness, 1 designates minimum trustworthiness and L designates maximum trustworthiness. The values between 0 and L represent intermediate trustworthiness levels TL, where a higher value implies higher trustworthiness.

At the time of production or personalization, the phone trustworthiness module 4 was loaded with the trustworthiness certificate 6 $\text{Cert}^{\text{ME}}_{\text{CA}}$, for example in X509 format or in WTLS format. The trustworthiness certificate 6 $\text{Cert}^{\text{ME}}_{\text{CA}}$ represents a binding between the name of the handheld phone 2, and a participant public key 7 K_{ME} , which binding is described in the trustworthiness certificate 6 $\text{Cert}^{\text{ME}}_{\text{CA}}$. The trustworthiness certificate 6 $\text{Cert}^{\text{ME}}_{\text{CA}}$ also contains an extension field 14 containing an integer which gives the trustworthiness level TL assigned to the handheld phone 2, where $0 \leq \text{TL} \leq L$. The trustworthiness certificate 6 bears trustworthiness certificate signature 9 from a certificate authority CA, which therefor used its certificate authority private key.

A participant private key 8 K^{-1}_{ME} associated with the participant public key 7 K_{ME} of the trustworthiness certificate 6 and functions that operate using that participant private key K^{-1}_{ME} are also loaded into the phone trustworthiness module 4 of the handheld phone 2, which module 4 is a secure and tamperproof processing area. Such an area should be used in all handheld phones with a trustworthiness level TL greater than 0. At least the participant private key 8 K^{-1}_{ME} need be securely stored, i.e. such that it can not be read by a non-allowed person or device.

Thus, the handheld phone 2 has assigned a participant public/private key pair 7, 8 $K_{\text{ME}}/K^{-1}_{\text{ME}}$ which can be used for verifying the affiliation or belonging of the trustworthiness certificate 6 to the handheld phone 2. The handheld phone 2 contains the signed trustworthiness certificate 6 that contains its participant public key 7 and also the trustworthiness level TL assigned to the handheld phone 2.

A certificate authority public key 17 corresponding to the certificate authority private key can be deemed to be publicly available, such that any entity can use it to check the

trustworthiness certificate signature 9 and therewith the affiliation of the handheld phone 2 and the trustworthiness certificate 6. Hence the trustworthiness level TL can be determined. Otherwise, the certificate authority might also provide the first communication partner 1 with this certificate authority public key 17, or it can be downloaded from somewhere, e.g. a data network.

At the time of production or personalization, a smartcard module 5 of the smartcard 1 is loaded with a first-partner certificate 10 $\text{Cert}^{\text{SC}}_{\text{CA}}$ designating a first-partner public key 11 K_{SC} for the smartcard 1 and a first-partner certificate signature 12. An associated first-partner private key 13 K^{-1}_{SC} is also loaded into the smartcard trustworthiness module 5, along with a collection 15 of three sample certificates C_1, C_2, C_3 of various certification authorities $\text{CA}_1, \text{CA}_2, \text{CA}_3$. Three sample certificates have been chosen for sake of exemplarity only. The collection 15 of sample certificates should generally be sufficiently large so that the trustworthiness certificate 6 $\text{Cert}^{\text{ME}}_{\text{CA}}$ presented by an arbitrary handheld phone 2 can be verified with very high probability. Here, a first sample certificate C_1 of the sample certificates C_1, C_2, C_3 contains the certificate authority public key 17 needed for authenticating or verifying the trustworthiness certificate signature 9.

When the smartcard 1 is now placed into the handheld phone 2, the trustworthiness level TL of the handheld phone 2 can be established as follows:

The smartcard 1 generates a random number R_1 and transmits it to the phone trustworthiness module 4 of the handheld phone 2. This is also called a challenge step, which is supposed to effect a response by the handheld phone 2.

The phone trustworthiness module 4 of the handheld phone 2 signs the random number R_1 with its participant private key 8 K^{-1}_{ME} , and returns the signature $\text{Sign}(R_1)$ for the random number R_1 together with its trustworthiness certificate 6 $\text{Cert}^{\text{ME}}_{\text{CA}}$ to the smartcard 1.

The smartcard 1 searches through its collection 15 of certificates C_1, C_2, C_3 to find the first sample certificate C_1 for the certificate authority CA, and verifies the trustworthiness certificate signature 9 on the received trustworthiness certificate 6 $\text{Cert}^{\text{ME}}_{\text{CA}}$. Concerning the collection 15 of certificates C_1, C_2, C_3 , it is possible to preload a preselection of such certificates on the smartcard 1 to cover the most popular certificate authorities CA. Whenever the trustworthiness certificate signature 9 does not have its equivalent certificate authority public key 17 and the thereto belonging certificate in the smartcard 1, the missing certificate

can be loaded from a source which provides this certificate, e.g. some network. It is usual that certificates are arranged in form of chains which means that for trusting a certificate its signature is to be tested wherefor a public key, embedded in another certificate is used, which other certificate is again signed, which signature is again to be checked, a.s.o. until one arrives at a definitely to be trusted certification authority, e.g. oneself. Also several of such certificate chains can exist.

If the trustworthiness certificate signature 9 is correct, the smartcard 1 then extracts the participant public key 7 K_{ME} from the trustworthiness certificate 6 $Cert^{ME}_{CA}$ and verifies therewith the random-number signature $Sign(R_1)$. The smartcard 1 aborts the process if either signature verification fails and establishes a trustworthiness level TL of 0.

If the verification succeeds, the smartcard 1 examines the trustworthiness field 14 in the trustworthiness certificate $Cert^{ME}_{CA}$ and constructs a trustworthiness level token (TLT) which indicates that the handheld phone 2 which is hosting the smartcard 1 has been authenticated by the smartcard 1 to the trustworthiness level TL.

The smartcard 1 has hence verified that the received trustworthiness certificate $Cert^{ME}_{CA}$ is valid in the sense that it was produced by an entity with the authority to assign the trustworthiness certificate $Cert^{ME}_{CA}$ and also that the trustworthiness certificate $Cert^{ME}_{CA}$ is not being replayed or imitated.

If the trustworthiness certificate 6 $Cert^{ME}_{CA}$ fails verification then the handheld phone 2 is considered untrusted, i.e. it is assigned a trustworthiness level TL of 0. In this case, the smartcard 1 may choose to terminate the session, or continue the session with the restriction that only applications which are allowed to run on the non-secure communication connection can be executed.

The smartcard 1 creates the trustworthiness level token TLT which represents the established trustworthiness level TL and forwards it to the second communication partner 3, which is a third party, to demonstrate to this third party the trustworthiness level TL of the handheld phone 2.

The smartcard 1 can communicate the established trustworthiness level TL to the second communication partner 3 by piggy-backing the trustworthiness level information TLT onto a communication message, signing this communication message with the first-partner private

key 13 and sending it to the second communication partner 3 where the signature can be tested by using the first-partner public key 11.

Alternatively, as e.g. used in GSM, the two communication partners 1, 3 can already trust each other before establishing the trustworthiness level TL of the participant 2 in that they both have a common private key, which could be the first-partner private key 13. This can be realized in that the smartcard 1 is issued by an authority which has set up the first-partner private key 13 in the server 3 and in that the smartcard is by this authority, which then of course is to be trusted, preloaded with the first-partner private key 13.

An application which uses contact to the back-end server 3 and which runs on the handheld phone 2 is selected for execution. The back-end server 3 and the smartcard 1 are authenticated to each other using a protocol that does not depend on the trustworthiness of the handheld phone 2. For example, if the handheld phone 2 is a GSM handset and the smartcard 1 is a SIM, then the back-end server 3 and the smartcard 1 are authenticated using the standard GSM authentication functions. Alternatively the authentication functions of WTLS can be used.

The smartcard 1 communicates the trustworthiness level TL of the handheld phone 2 to the back-end server 3 by appending the trustworthiness level token TLT to the application packets of the application that are sent from the smartcard 1 to the back-end server 3. The trustworthiness level token TLT may be appended to each application packet or be transmitted according to another strategy, depending on a determined token communication policy, e.g. once per a fixed time period or a fixed number of times per session etc.

When the back-end server 3 has received the trustworthiness level token TLT of the handheld phone 2 via the smartcard 1, it need not verify the trustworthiness level TL of the handheld phone 2 with the handheld phone 2 itself, because this has already been done by the trusted smartcard 1. For the application A the back-end server 3 consults a trustworthiness policy 16 pol(A), e.g. in form of a stored table, which describes what restrictions are placed on the application A relative to the trustworthiness level TL designated by the trustworthiness level token TLT. The back-end server 3 adjusts its actions and responses in the application A accordingly. With other words, the back-end server 3 consults the trustworthiness policy 16 pol(A) for the application A, and modifies or chooses its communication

Revised Claims

1. Method of establishing a trustworthiness level (TL) of a participant (2) in a communication connection between a first communication partner (1) and a second communication partner (3) and for adapting communication behavior to the established trustworthiness level (TL), whereby said participant (2) is equipped with a trustworthiness certificate (6) and a therefrom separated securely stored participant private key (8) and that said first communication partner (1) receives said trustworthiness certificate (6) from said participant (2), where from said trustworthiness level (TL) is derived and established and said first communication partner (1) tests whether said trustworthiness certificate (6) belongs to said participant (2) by using a participant public key (7) which corresponds to the participant private key (8) and that in case said trustworthiness certificate (6) is confirmed by said test to belong to said participant (2), said first communication partner (1) communicates said established trustworthiness level (TL) to said second communication partner (3) and that at least one parameter of said communication behavior is chosen in dependence of said established trustworthiness level (TL).
2. Method according to claim 1, characterized in that the trustworthiness certificate (6) arrives at the first communication partner (1) signed with a signature (9), produced with a certificate authority private key, and that said first communication partner (1) authenticates said signature (9) using a certificate authority public key (17).
3. Method according to claim 1, characterized in that the certificate authority public key (17) is read from a storage of the first communication partner (1).
4. Method according to claim 1, characterized in that the first communication partner (1) communicates the established trustworthiness level (TL) to the second communication partner (2) by piggy-backing a trustworthiness level information (TLT) onto a communication message, signing said communication message with a first-partner private key (13) and sending it to said second communication partner (3).

5. Method according to claim 1, characterized in that the authenticity of the trustworthiness level information (TLT) of the communication message is testable by the second communication partner (3) by using a first-partner public key (11).
- 5 6. Method according to claim 1, characterized in that as one of the parameters of the communication behavior which is chosen in dependence of the established trustworthiness level (TL), is chosen the amount or number of a valuable asset, preferably a maximum number of financial transactions and/or a maximum financial value of a financial transaction and/or a maximum number of confidential words.
- 10 7. Method according to claim 1, characterized in that the test whether the trustworthiness certificate (6) belongs to the participant (2) is performed in that a test number (R_1) is transmitted by the first communication partner (1) to said participant (2) from where said test number (R_1) returns signed under use of the participant private key (8) and in that the signature of the returning test number (R_1) is verified by using a participant public key (7) which corresponds to said participant private key (8).
- 15 8. Method according to claim 1, characterized in that the participant public key (7) is received by the first communication partner (1) as content of the trustworthiness certificate (6).
- 20 9. Method according to claim 1, characterized in that the trustworthiness level (TL) is established in that for each trustworthiness level (TL) a different trustworthiness certificate (6) with a corresponding pair of participant public key (7) and participant private key (8) is used.

10. Method of establishing the trustworthiness level (TL) of a participant (2) in a communication connection between a first communication partner (1) and a second communication partner (3) and for adapting communication behavior to the established trustworthiness level (TL), whereby said participant (2) is equipped with a securely stored participant private key (8) and that said first communication partner (1) performs an authentication test by using a participant public key (7) which corresponds to the participant private key (8) which also leads to establishing said trustworthiness level (TL) and that in case of a successful authentication said first communication partner (1) communicates the established trustworthiness level (TL) to said second communication partner (3) and that at least one parameter of said communication behavior is chosen in dependence of said established trustworthiness level (TL).
11. that the authentication test is performed in that a test number (R_1) is transmitted by the first communication partner (1) to the participant (2) from where said test number (R_1) returns signed under use of the participant private key (8) and in that the signature of the returning test number (R_1) is verified by using a participant public key (7) which corresponds to said participant private key (8).

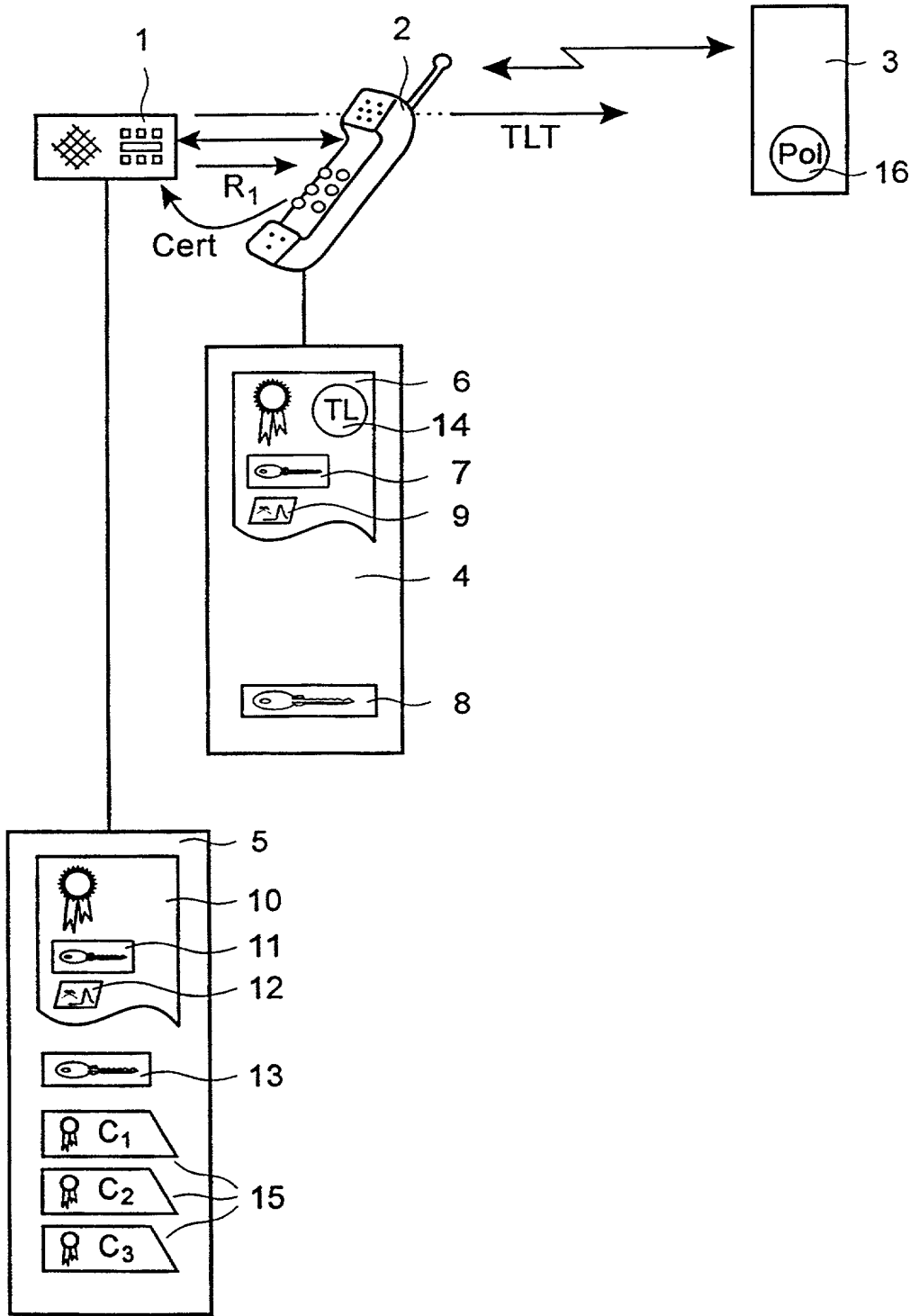


Fig. 1

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled;

METHOD OF ESTABLISHING THE TRUSTWORTHINESS OF A PARTICIPANT IN A COMMUNICATION CONNECTION

the specification of which (check one)

☐ is attached hereto.

☒ was filed on 23 November 1998 as United States Application No. _____ or

PCT International Application No. PCT/IB98/01854 and

was amended on 30 August 2000 (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed
<u>98113121.2</u> (Number)	<u>EP</u> (Country)	<u>15/July/1998</u> (Day/Month/Year Filed)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	<input type="checkbox"/> Yes <input type="checkbox"/> No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	<input type="checkbox"/> Yes <input type="checkbox"/> No

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below.

_____ (Application Number)	_____ (Filing Date)
_____ (Application Number)	_____ (Filing Date)

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

I hereby claim the benefit under 35 U.S.C. §120 of any United States Application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States, or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in 37 CFR §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
--------------------------	---------------	---

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
--------------------------	---------------	---

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith (list name and registration number).

Manny W. Schecter (Reg. 31,722), Lauren C. Bruzzone (Reg. 35,082), Christopher A. Hughes (Reg. 26,914), Edward A. Pennington (Reg. 32,588), John E. Hoel (Reg. 26,279), Joseph C. Redmond, Jr. (Reg. 18,753), Richard M. Ludwin (Reg. 33,010), Marc A. Erlich (Reg. 39,966), Douglas W. Cameron (Reg. 31,596), Louis P. Herzberg (Reg. 41,500), Marian Underweiser (Reg. 46,134), Stephen C. Kaufman (Reg. 29,551), Daniel P. Morris (Reg. 32,053), Louis J. Parcello (Reg. 33,206), Robert M. Trepp (Reg. 25,933), Gail H. Zarick (Reg. 43,303), Robert P. Tassinari, Jr. (Reg. 36,030), Paul J. Otterstedt (Reg. 37,411) and Derek S. Jennings (Reg. No. 41,473)

Send Correspondence to: PERENCE & ASSOCIATES, 129 Oakhurst Road, Pittsburgh, PA 15215

Direct Telephone Calls to: (name and telephone number) Stanley D. Ference III, (412) 781-7386

Carl Binding

Full name of sole or first inventor

Inventor's Signature

Date

Russistrasse 7, CH-8800 Thalwil, Switzerland

Residence

Switzerland

Citizenship

Same as above

Post Office Address

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

Stefan Hild

Full name of second joint inventor, if any

Inventor's Signature

Date

89 Mitchell Road, Somers, NY 10589, USA
Residence

Germany
Citizenship

Same as above
Post Office Address

Michael Moser

Full name of third joint inventor, if any

Inventor's Signature

Date

Froburgstrasse 19, CH-8006 Zurich, Switzerland
Residence

Austria
Citizenship

Same as above
Post Office Address

Luke O'Connor

Full name of fourth joint-inventor, if any

Inventor's Signature

Date

Sihlhof 16, CH-8134 Adliswil, Switzerland
Residence

Australia
Citizenship

Same as above
Post Office Address

3-444760-100000

4-00

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD OF ESTABLISHING THE TRUSTWORTHINESS OF A PARTICIPANT IN A COMMUNICATION CONNECTION

the specification of which (check one)

☐ is attached hereto.

☒ was filed on 23 November 1998 as United States Application No. _____ or
PCT International Application No. PCT/IB98/01854 and
was amended on 30 August 2000 (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed
<u>98113121.2</u> (Number)	<u>EP</u> (Country)	<u>15/July/1998</u> (Day/Month/Year Filed)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	<input type="checkbox"/> Yes <input type="checkbox"/> No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	<input type="checkbox"/> Yes <input type="checkbox"/> No

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below.

_____ (Application Number)	_____ (Filing Date)
_____ (Application Number)	_____ (Filing Date)

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

I hereby claim the benefit under 35 U.S.C. §120 of any United States Application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States, or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in 37 CFR §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)

(Filing Date)

(Status) (patented, pending, abandoned)

(Application Serial No.)

(Filing Date)

(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith (list name and registration number).

Manny W. Schecter (Reg. 31,722), Lauren C. Bruzzone (Reg. 35,082), Christopher A. Hughes (Reg. 26,914), Edward A. Pennington (Reg. 32,588), John E. Hoel (Reg. 26,279), Joseph C. Redmond, Jr. (Reg. 18,753), Richard M. Ludwin (Reg. 33,010), Marc A. Erlich (Reg. 39,966), Douglas W. Cameron (Reg. 31,596), Louis P. Herzberg (Reg. 41,500), Marian Underweiser (Reg. 46,134), Stephen C. Kaufman (Reg. 29,551), Daniel P. Morris (Reg. 32,053), Louis J. Percello (Reg. 33,206), Robert M. Trepp (Reg. 25,933), Gail H. Zarick (Reg. 43,303), Robert P. Tassinari, Jr. (Reg. 36,030), Paul J. Otterstedt (Reg. 37,411) and Derek S. Jennings (Reg. No. 41,473)

Send Correspondence to: FERENCE & ASSOCIATES, 129 Oakhurst Road, Pittsburgh, PA 15215

Direct Telephone Calls to: (name and telephone number) Stanley D. Ference III, (412) 781-7386

Carl Binding

Full name of sole or first inventor

Inventor's Signature

Date

Russistrasse 7, CH-8800 Thalwil, Switzerland
Residence

Switzerland
Citizenship

Same as above
Post Office Address

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

2.6
Stefan Hild

Full name of second joint inventor, if any


Inventor's Signature

8/8/01
Date

Austrasse 27, CH-8134 Adliswil, Switzerland
Residence

CH4

Germany
Citizenship

Same as above
Post Office Address

Michael Moser

Full name of third joint inventor, if any

Inventor's Signature

Date

Froburgstrasse 19, CH-8006 Zurich, Switzerland
Residence

Austria
Citizenship

Same as above
Post Office Address

Luke O'Conner

Full name of fourth joint-inventor, if any

Inventor's Signature

Date

Sihlhof 16, CH-8134 Adliswil, Switzerland
Residence

Australia
Citizenship

Same as above
Post Office Address